



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/639,943	08/13/2003	Richard H. Boivie	YOR920030260US1 (16780)	6976
23389 7590 12/31/2008 SCULLY SCOTT MURPHY & PRESSER, PC 400 GARDEN CITY PLAZA SUITE 300 GARDEN CITY, NY 11530			EXAMINER LANIER, BENJAMIN E	
			ART UNIT 2432	PAPER NUMBER
			MAIL DATE 12/31/2008	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

DETAILED ACTION

Response to Arguments

1. Applicant argues, "While Col. 8, lines 46-69 and Col. 14, lines 59-64 appear to say that the check values are 'saved for later use and/or transmission', that passage is not disclosing or suggesting that only its sender keeps the check values. Rather, it is save for later use, i.e., for sending it to the receiver." This argument is not persuasive because Applicant is referring to the alternative embodiment where the check values are transmitted (and/or transmission). Applicant has chosen to ignore the very clear fact that Serret-Avila specifically discloses that the check values can be stored without transmission.

2. Applicant alleges that "Serret-Avila's method would not work if its check values and signatures were kept only with the sender." However, this allegation is wholly unsupported by any evidence.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.

Art Unit: 2432

4. Considering objective evidence present in the application indicating obviousness or nonobviousness.
5. Claims 1, 2, 12-15, 25, 26, 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Burns, U.S. Patent No. 6,405,315, in view of Serret-Avila, U.S. Patent No. 6,959,384.
Referring to claims 1, 14, 25, 33, Burns discloses a decentralized remotely encrypted file system wherein a network storage device is used to store encrypted files for network clients (Figure 2 & Col. 3, lines 44-52 & Col. 5, lines 25-45), which meets the limitation of a network-attached storage device for storing encrypted data. A network client must encrypt the data prior to transmission to the network storage device for storage (Col. 3, lines 49-52 & Col. 5, lines 40-45), which meets the limitation of means at a client device for encrypting data prior to sending data blocks to said network-attached storage device. The encrypted data includes a hash of the data to detect corruption or unauthorized changes to the data (Figure 5 & Col. 8, lines 5-10), which meets the limitation of said encrypting means protecting confidentiality and integrity of data blocks sent to said network-attached storage device, means at said client device for generating an integrity value corresponding to one or more data blocks, said integrity value comprising information for preventing modification, relocation and replay of data for each data block sent to said network-attached storage device, means for storing said integrity values of one or more data blocks. When a client requests access to the stored data, the data is sent to the network client, decrypted, hashed, and verified by comparing the calculated hash with the previously calculated hashed that was stored with the data (Col. 8, lines 5-10 & Col. 10, line 60 – Col. 11, line 17), which meets the limitation of means at said client device for receiving and decrypting data blocks received from said network-attached storage device, means for performing an integrity check at said client device utilizing stored integrity values corresponding to one or more said

Art Unit: 2432

data blocks received from said network-attached storage device, wherein said integrity check protects the integrity of data blocks stored in said network-attached storage devices, storing said integrity value on the client device where said integrity value was generated. Burns discloses that the encrypted data includes a hash of the data to detect corruption or unauthorized changes to the data (Figure 5 & Col. 8, lines 5-10), but does not disclose that the hash is stored at the client device instead of transmitting the hash with the encrypted data. Serret-Avila discloses that the hash tree can be maintained by the client device or stored in network storage (Col. 8, lines 46-69 & Col. 14, lines 59-64), which meets the limitation of said root data structure is not written out to the storage device. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the client device of Burns to maintain the hash information instead of transmitting it with the encrypted data in order to provide a faster means of data verification upon access as taught by Serret-Avila (Col. 16, line 64 – Col. 17, line 17). Burns does not disclose using integrity trees stored on the client device to verify the integrity of the stored data. Serret-Avila discloses a method and system for authenticating the integrity of data wherein the data has a corresponding hash tree associated with it for authentication (Col. 15, lines 56-60), which meets the limitation of means for storing further includes means for generating an integrity tree structure, said integrity tree structure storing integrity values corresponding to each disk block written to said storage device. When the user attempts to access the data, relevant branches of the hash tree, including the root, are loaded into the memory of the user computer (Col. 15, lines 62-67), which meets the limitation of wherein said integrity tree comprises a hierarchical data structure, said hierarchical data structure including two or more layers of integrity data structures, wherein a top layer of said hierarchical data structure includes a root

Art Unit: 2432

data structure for protecting integrity of all content written to said storage device, and said root data structure is stored on the client device, wherein contents of said integrity tree are updated and verified on said client device. Authentication of the hashes require hashing the hashes at a particular level to yield the hashes for the next level, which are compared with the actual hashes that correspond to that next level (Col. 17, lines 35-53), which meets the limitation of each successive layer of integrity data structures including meta-data protecting integrity of data at an immediate prior layer. It would have been obvious to one of ordinary skill in the art at the time the invention was made for integrity verification of Burns to use the hash trees described in Serret-Avila in order to enable the user to verify the data on-the-fly, thus obviating the need to process the entire data object before it can be verified as taught in Serret-Avila (Col. 6, lines 31-36).

Referring to claims 2, 15, 26, Burns discloses a network client must encrypt the data prior to transmission to the network storage device for storage (Col. 3, lines 49-52 & Col. 5, lines 40-45), which meets the limitation of encryption means generates encrypted cipher text data blocks that are a function of plaintext data included in said data block and a first encryption key.

Referring to claim 12, Burns discloses that the network storage device includes disk drives for storage (Col. 5, lines 7-8), which meets the limitation of said storage device comprises non-volatile storage.

Referring to claim 13, Burns discloses that the network storage device is remotely located from said client device, said encrypted blocks being written across a network link (Figure 1).

6. Claims 3, 7-8, 10, 11, 16, 20, 21, 23, 24, 27, 29-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Burns, U.S. Patent No. 6,405,315, in view of Serret-Avila, U.S. Patent

Art Unit: 2432

No. 6,959,384 as applied to claims 1, 2, 14, 25 above, and further in view of Pang, U.S. Patent No. 6,931,543, in view of Tatebayashi, U.S. Patent No. 5,124,117. Referring to claims 3, 16, 27, Burns discloses a decentralized remotely encrypted file system wherein a network storage device is used to store encrypted files for network clients (Figure 2 & Col. 3, lines 44-52 & Col. 5, lines 25-45). Burns discloses that timestamps are included and associated with the encrypted data to identify when the data was last modified and/or accessed (Figure 5 & Col. 12, lines 66-67).

Burns does not disclose utilizing an address location for the data or a version number that indicates a block write increment in the encryption process. Pang discloses a programmable logic device for decrypting data that utilizes address information for the encryption and decryption of the data (Col. 3, lines 57-62), which meets the limitation of said encryption means implements a whitening value which is a function of a second encryption key, an address location for said storage block, said encryption means further generating cipher text data blocks that are additionally a function of said whitening value. Tatebayashi discloses a cryptographic system wherein timestamps are utilized in the encryption process of data (Col. 14, lines 11-15), which meets the limitation of encryption means implements a whitening value which is a function of a version number indicating a block write increment. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the location address information of the data and timestamps, as it is stored in the network storage device in Burns, in order to prevent attacks that relocate portions of the encrypted bitstream such that when they are unencrypted they are placed into visible portions of the device not intended by the designer as taught by Pang (Col. 3, lines 55-58) and to prevent attacking users from listening to

Art Unit: 2432

communications and conspiring to obtain the encryption key as taught by Tatebayashi (Col. 13, lines 9-31 & Col. 14, lines 11-15).

Referring to claims 7, 8, 20, 21, 29, Burns discloses that the entries of the file structure also contain meta data (Col. 2, lines 30-33 & Col. 5, lines 25-28). Burns does not disclose utilizing an address location for the data or a version number that indicates a block write increment in the encryption process. Pang discloses a programmable logic device for decrypting data that utilizes address information for the encryption and decryption of the data (Col. 3, lines 57-62), which meets the limitation of said encryption means implements a whitening value which is a function of a second encryption key, an address location for said storage block, said encryption means further generating cipher text data blocks that are additionally a function of said whitening value. Tatebayashi discloses a cryptographic system wherein timestamps are utilized in the encryption process of data (Col. 14, lines 11-15), which meets the limitation of said hierarchical data structure includes said written encrypted data blocks at a first layer, and a succeeding layer of meta data blocks, each meta data block including data structures representing a plurality of disk blocks written at said first layer, each meta data block data structure comprising an integrity value and a version number pair for each of said plurality of disk blocks, said integrity tree includes a succeeding layer of higher level meta data blocks for protecting a layer of meta data blocks below, each higher level meta data block comprising data structures representing a plurality of meta data blocks, each higher level meta data block data structure comprising an integrity value and version number pair generated for each of said plurality of meta data blocks. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the location address information of the data and timestamps, as it

Art Unit: 2432

is stored in the network storage device in Burns, in order to prevent attacks that relocate portions of the encrypted bitstream such that when they are unencrypted they are placed into visible portions of the device not intended by the designer as taught by Pang (Col. 3, lines 55-58) and to prevent attacking users from listening to communications and conspiring to obtain the encryption key as taught by Tatebayashi (Col. 13, lines 9-31 & Col. 14, lines 11-15).

Referring to claims 10, 11, 23, 24, 30-32, Burns discloses that the file system data can be updated (Col. 5, lines 40-45), means comparing integrity of data blocks to be read on a path from said root data structure via successive higher meta data blocks and meta data block layers until a desired data block at a first layer is read. Burns does not disclose utilizing an address location for the data or a version number that indicates a block write increment in the encryption process. Pang discloses a programmable logic device for decrypting data that utilizes address information for the encryption and decryption of the data (Col. 3, lines 57-62), which meets the limitation of said encryption means implements a whitening value which is a function of a second encryption key, an address location for said storage block, said encryption means further generating cipher text data blocks that are additionally a function of said whitening value. Tatebayashi discloses a cryptographic system wherein timestamps are utilized in the encryption process of data (Col. 14, lines 11-15), which meets the limitation of writing a data block to said storage device, said writing including updating a written data block's version number and checksum in the associated meta data blocks, and, said checksum and version number value updating being performed at each successive meta data layer corresponding to said written data block, including updating performed at said root data structure. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the location address information of the data and

Art Unit: 2432

timestamps, as it is stored in the network storage device in Burns, in order to prevent attacks that relocate portions of the encrypted bitstream such that when they are unencrypted they are placed into visible portions of the device not intended by the designer as taught by Pang (Col. 3, lines 55-58) and to prevent attacking users from listening to communications and conspiring to obtain the encryption key as taught by Tatebayashi (Col. 13, lines 9-31 & Col. 14, lines 11-15).

7. Claims 4, 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Burns, U.S. Patent No. 6,405,315, in view of Serret-Avila, U.S. Patent No. 6,959,384 as applied to claims 1, 2, 14, 15 above, and further in view of Aiello, U.S. Patent No. 5,608,801. Referring to claims 4, 17, Burns discloses a decentralized remotely encrypted file system wherein a network storage device is used to store encrypted files for network clients (Figure 2 & Col. 3, lines 44-52 & Col. 5, lines 25-45). Burns does not disclose using DES or AES encryption. It would have been obvious to one of ordinary skill in the art at the time the invention was made to utilize the DES algorithm to encrypt the data of Burns because DES provides a reasonable fast and commercially available encryption algorithm as taught in Aiello (Col. 3, lines 55-57).

Conclusion

8. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

Art Unit: 2432

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to BENJAMIN E. LANIER whose telephone number is (571)272-3805. The examiner can normally be reached on M-Th 7:00am-5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Benjamin E Lanier/
Primary Examiner, Art Unit 2432